

#3

PATENT

81942.0004

Express Mail Label No. EL 589 806 385 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kiyoshi OGISHI et al.

Serial No: Not assigned

Filed: November 7, 2000

For: KEY SHARING METHOD, SECRET KEY  
GENERATING METHOD, COMMON KEY  
GENERATING METHOD AND CRYPTOGRAPHIC  
COMMUNICATION METHOD IN ID-NIKS  
CRYPTOSYSTEM

Art Unit: Not assigned

Examiner: Not assigned

JC930 U.S. PTO  
09/708263  
11/07/00

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION

Assistant Commissioner for Patents

Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-133471 which was filed May 2, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

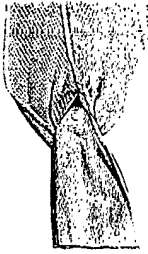
HOGAN & HARTSON L.L.P.

Date: November 7, 2000

By: 

Louis A. Mok  
Registration No. 22,585  
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900  
Los Angeles, California 90071  
Telephone: 213-337-6700  
Facsimile: 213-337-6701



BEST AVAILABLE COPY

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

JCS30 U.S. PTO  
09/708263  
11/04/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日

Date of Application:

2000年 5月 2日

出 願 番 号

Application Number:

特願2000-133471

出 願 人

Applicant (s):

村田機械株式会社

境 隆一

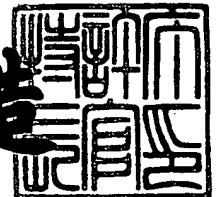
笠原 正雄

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 8月18日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 21117

【特記事項】 特許法第 3 0 条第 1 項の規定の適用を受けようとする特  
許出願

【提出日】 平成12年 5月 2日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00  
H04L 9/00

【発明の名称】 鍵共有方法, 秘密鍵生成方法, 共通鍵生成方法, 暗号通  
信方法, 秘密鍵生成器, 共通鍵生成器, 暗号通信システ  
ム及び記録媒体

【請求項の数】 18

【発明者】

【住所又は居所】 京都府京都市山科区大宅辻脇町 3 7 番地の 3 2

【氏名】 大岸 聖史

【発明者】

【住所又は居所】 京都府京都市山科区安朱東海道町 1 6 - 2 緑山荘 B 棟 1  
0 1 号室

【氏名】 境 隆一

【発明者】

【住所又は居所】 大阪府箕面市粟生外院 4 丁目 1 5 番 3 号

【氏名】 笠原 正雄

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【識別番号】 599100556

【氏名又は名称】 境 隆一

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 鍵共有方法，秘密鍵生成方法，共通鍵生成方法，暗号通信方法，秘密鍵生成器，共通鍵生成器，暗号通信システム及び記録媒体

【特許請求の範囲】

【請求項 1】 エンティティ自身の秘密鍵と相手エンティティの公開鍵とを用いて予備通信なしに鍵共有を行う方法において、前記相手エンティティを特定する特定情報に基づき代数曲線上の点に写像したものを前記公開鍵とすることを特徴とする鍵共有方法。

【請求項 2】 両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、代数曲線上で定義されるペアリングを使用することを特徴とする鍵共有方法。

【請求項 3】 両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、一方のエンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とから生成された秘密鍵と、他方のエンティティの特定情報に基づき前記代数曲線上の点に写像してなる公開鍵とを用い、前記楕円曲線上で定義されるペアリングを使用して鍵共有を行うことを特徴とする鍵共有方法。

【請求項 4】 前記ペアリングは、バイユペアリングまたはテイトペアリングである請求項 2 または 3 記載の鍵共有方法。

【請求項 5】 前記代数曲線はその上で定義される離散対数問題を多項式時間で解くことができない請求項 1 ～ 4 の何れかに記載の鍵共有方法。

【請求項 6】 一方のエンティティと他方のエンティティとで鍵共有を行う際の夫々のエンティティでの演算処理の過程にあって、互いに逆数の関係になる数値を生成し合う請求項 1 ～ 5 の何れかに記載の鍵共有方法。

【請求項 7】 前記各エンティティの特定情報に基づいて複数の公開鍵を生成する請求項 1 ～ 6 の何れかに記載の鍵共有方法。

【請求項 8】 エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを

特徴とする秘密鍵生成方法。

【請求項 9】 エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に対して一方方向性関数を作用させた値に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項 10】 第 1 エンティティを特定する特定情報に基づく秘密鍵と通信相手の第 2 エンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する方法において、前記第 1 エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて前記秘密鍵を生成し、前記第 2 エンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵とすることを特徴とする共通鍵生成方法。

【請求項 11】 前記代数曲線上で定義されるペアリングを使用して前記共通鍵を生成する請求項 10 記載の共通鍵生成方法。

【請求項 12】 請求項 6 記載の鍵共有方法に基づいて共通鍵を生成する方法であって、前記数値における逆数の関係を利用して共通鍵を生成することを特徴とする共通鍵生成方法。

【請求項 13】 センタから各エンティティへ各エンティティの秘密鍵を送付し、一方のエンティティが前記センタから送付された自身の秘密鍵と他方のエンティティの公開鍵とから求めた共通鍵を用いて平文を暗号文に暗号化して前記他方のエンティティへ伝送し、前記他方のエンティティが伝送された暗号文を、前記センタから送付された自身の秘密鍵と前記一方のエンティティの公開鍵とから求めた、前記共通鍵と同一の共通鍵を用いて平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、各エンティティを特定する特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティの特定情報に基づき代数曲線上の点に写像したものを各エンティティの公開鍵とすることを特徴とする暗号通信方法。

【請求項 14】 エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する生成器において、前記エンティティの特定情報に基づき

代数曲線上の点に写像して写像値を得る手段と、該写像値と秘密情報とを用いて前記秘密鍵を生成する手段とを備えることを特徴とする秘密鍵生成器。

【請求項 1 5】 一方のエンティティを特定する特定情報に基づく秘密鍵と通信相手の他方のエンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する生成器において、前記他方のエンティティの特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得る手段と、該写像値と前記秘密鍵とを用いて前記共通鍵を生成する手段とを備えることを特徴とする共通鍵生成器。

【請求項 1 6】 送信すべき情報である平文を暗号文に暗号化する暗号化处理、及び、送信された暗号文を平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティを特定する特定情報に基づいて各エンティティの秘密鍵を生成して各エンティティへ送付するセンタと、該センタから送付された自身の秘密鍵と通信対象のエンティティの特定情報に基づく公開鍵とを用いて前記暗号化处理及び復号処理に使用する共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、前記センタにて、各エンティティの特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティにて、通信対象のエンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵として前記共通鍵を生成するようにしたことを特徴とする暗号通信システム。

【請求項 1 7】 コンピュータにエンティティの秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と秘密情報とを用いて前記秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする記録媒体。

【請求項 1 8】 コンピュータに、暗号通信システムにおける平文から暗号文への暗号化处理及び暗号文から平文への復号処理に使用する共通鍵を第 1 エンティティ側で生成させるためのプログラムが記録されているコンピュータでの読

み取りが可能な記録媒体において、前記第 1 エンティティの秘密鍵を入力することをコンピュータに実行させるプログラムコード手段と、通信相手の第 2 エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と入力した前記秘密鍵とを用いて前記共通鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、予備通信なしで両エンティティ間で共通鍵を共有し合う鍵共有方法、センタにて各エンティティ固有の秘密鍵を生成する秘密鍵生成方法及び秘密鍵生成器、各エンティティで暗号化処理・復号処理に必要な共通鍵を生成する共通鍵生成方法及び共通鍵生成器、情報の内容が当事者以外にはわからないように暗号文にて通信を行う暗号通信方法及び暗号通信システム、並びに、これらの方法を行うためのプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換するこ



とである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

## 【 0 0 0 4 】

暗号化鍵と復号鍵とは、等しくても良いし、異なっても良い。両者の鍵が等しい暗号系は、共通鍵暗号系と呼ばれ、米国商務省標準局が採用した D E S （Data Encryption Standards）はその典型例である。また、両者の鍵が異なる暗号系の一例として、公開鍵暗号系と呼ばれる暗号系が提案された。この公開鍵暗号系は、暗号系を利用する各ユーザ（エンティティ）が暗号化鍵と復号鍵とを一对一ずつ作成し、暗号化鍵を公開鍵リストにて公開し、復号鍵のみを秘密に保持するという暗号系である。公開鍵暗号系では、この一对となる暗号化鍵と復号鍵とが異なり、一方向性関数を利用することによって暗号化鍵から復号鍵を割り出せないという特徴を持たせている。

## 【 0 0 0 5 】

公開鍵暗号系は、暗号化鍵を公開するという画期的な暗号系であって、高度情報化社会の確立に必要な上述した 3 つの要素に適合するものであり、情報通信技術の分野等での利用を図るべく、その研究が活発に行われ、典型的な公開鍵暗号系として R S A 暗号系が提案された。この R S A 暗号系は、一方向性関数として素因数分解の困難さを利用して実現されている。また、離散対数問題を解くことの困難さ（離散対数問題）を利用した公開鍵暗号系も種々の手法が提案されてきた。

## 【 0 0 0 6 】

また、各エンティティの住所、氏名、電子メールのアドレス等の個人を特定する I D （Identity）情報を利用する暗号系が提案された。この暗号系では、I D 情報に基づいて送受信者間で共通の暗号化・復号鍵を生成する。また、この I D

情報に基づく暗号技法には、(1) 暗号文通信に先立って送受信者間での予備通信を必要とする方式と、(2) 暗号文通信に先立って送受信者間での予備通信を必要としない方式とがある。特に、(2) の手法は予備通信が不要であるので、エンティティの利便性が高く、将来の暗号系の中樞をなすものと考えられている。

## 【0007】

この(2)の手法による暗号系は、ID-NIKS (ID-based non-interactive key sharing scheme)と呼ばれており、通信相手のID情報を用いて予備通信を行うことなく暗号化・復号鍵を共有する方式を採用している。ID-NIKSは、送受信者間で公開鍵、秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行える。

## 【0008】

図4は、このID-NIKSのシステムの原理を示す図である。信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。図4において、エンティティXの特定情報であるエンティティXの名前、住所、電話番号、メールアドレス等のID情報を $\{ID_X\}$ で表す。センタは任意のエンティティXに対して、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びエンティティXのID情報 $\{ID_X\}$ に基づいて、以下のように秘密情報 $S_{Xi}$ を計算し、秘密裏にエンティティXへ配布する。

$$S_{Xi} = F_i (\{SC_i\}, \{PC_i\}, \{ID_X\})$$

## 【0009】

エンティティXは他の任意のエンティティYとの間で、暗号化、復号のための共通鍵 $K_{XY}$ を、エンティティX自身の秘密情報 $\{S_{Xi}\}$ 、センタ公開情報 $\{PC_i\}$ 及び相手先のエンティティYのID情報 $\{ID_Y\}$ を用いて以下のように生成する。

$$K_{XY} = f (\{S_{Xi}\}, \{PC_i\}, \{ID_Y\})$$

また、エンティティYも同様にエンティティXへの鍵を共通鍵 $K_{YX}$ を生成する。もし常に $K_{XY} = K_{YX}$ の関係が成立すれば、この鍵 $K_{XY}$ 、 $K_{YX}$ をエンティティX、

Y 間で暗号化鍵、復号鍵として使用できる。

【0010】

上述した公開鍵暗号系では、例えばRSA暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ID-NIKSでは、各ID情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。従って、図4に示すようなID-NIKSのシステムが安全に実現されれば、多数のエンティティが加入するコンピュータネットワーク上で便利な暗号系を構築できる。このような理由により、ID-NIKSが将来の暗号系の中心になると期待されている。

【0011】

【発明が解決しようとする課題】

通信相手のID情報を用いて予備通信を行うことなく暗号化鍵及び復号鍵となる共通鍵を互いに共有するようなID-NIKSにあっては、特に複数のエンティティが結託する結託攻撃に対して十分に安全であることが望まれる。そして、暗号学的に安全なID-NIKSを構築できるか否かは、高度情報化社会にとって重要な問題であり、より理想的な暗号方式の探究が進められている。

【0012】

本発明は斯かる事情に鑑みてなされたものであり、各エンティティの特定情報（ID情報）に基づいて、楕円暗号で利用されている楕円曲線等の代数曲線上の点に写像することにより、予備通信を行うことなく両エンティティ間で容易に共通鍵を共有し合える鍵共有方法、この鍵共有方法に基づいて安全なID-NIKSを構築できるための秘密鍵生成方法及び秘密鍵生成器、共通鍵生成方法及び共通鍵生成器、暗号通信方法及び暗号通信システム、並びに、これらの方法を行うためのプログラムを記録した記録媒体を提供することを目的とする。

【0013】

【課題を解決するための手段】

請求項1に係る鍵共有方法は、エンティティ自身の秘密鍵と相手エンティティの公開鍵とを用いて予備通信なしに鍵共有を行う方法において、前記相手エンティティを特定する特定情報に基づき代数曲線上の点に写像したものを前記公開鍵

とすることを特徴とする。

【 0 0 1 4 】

請求項 2 に係る鍵共有方法は、両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、代数曲線上で定義されるペアリングを使用することを特徴とする。

【 0 0 1 5 】

請求項 3 に係る鍵共有方法は、両エンティティを夫々特定する特定情報に基づき前記両エンティティ間で予備通信なしに鍵共有を行う方法において、一方のエンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とから生成された秘密鍵と、他方のエンティティの特定情報に基づき前記代数曲線上の点に写像してなる公開鍵とを用い、前記楕円曲線上で定義されるペアリングを使用して鍵共有を行うことを特徴とする。

【 0 0 1 6 】

請求項 4 に係る鍵共有方法は、請求項 2 または 3 において、前記ペアリングは、バイユペアリングまたはテイトペアリングであることを特徴とする。

【 0 0 1 7 】

請求項 5 に係る鍵共有方法は、請求項 1 ～ 4 の何れかにおいて、前記代数曲線はその上で定義される離散対数問題を多項式時間で解くことができないことを特徴とする。

【 0 0 1 8 】

請求項 6 に係る鍵共有方法は、請求項 1 ～ 5 の何れかにおいて、一方のエンティティと他方のエンティティとで鍵共有を行う際の夫々のエンティティでの演算処理の過程にあって、互いに逆数の関係になる数値を生成し合うことを特徴とする。

【 0 0 1 9 】

請求項 7 に係る鍵共有方法は、請求項 1 ～ 6 の何れかにおいて、前記各エンティティの特定情報に基づいて複数の公開鍵を生成することを特徴とする。

【 0 0 2 0 】

請求項 8 に係る秘密鍵生成方法は、エンティティを特定する特定情報に基づい

て前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを特徴とする。

## 【 0 0 2 1 】

請求項 9 に係る秘密鍵生成方法は、エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する方法において、前記エンティティの特定情報に対して一方向性関数を作用させた値に基づき代数曲線上の点に写像したものと秘密情報とを用いて、前記秘密鍵を生成することを特徴とする。

## 【 0 0 2 2 】

請求項 1 0 に係る共通鍵生成方法は、第 1 エンティティを特定する特定情報に基づく秘密鍵と通信相手の第 2 エンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する方法において、前記第 1 エンティティの特定情報に基づき代数曲線上の点に写像したものと秘密情報とを用いて前記秘密鍵を生成し、前記第 2 エンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵とすることを特徴とする。

## 【 0 0 2 3 】

請求項 1 1 に係る共通鍵生成方法は、請求項 1 0 において、前記代数曲線上で定義されるペアリングを使用して前記共通鍵を生成することを特徴とする。

## 【 0 0 2 4 】

請求項 1 2 に係る共通鍵生成方法は、請求項 6 記載の鍵共有方法に基づいて共通鍵を生成する方法であって、前記数値における逆数の関係を利用して共通鍵を生成することを特徴とする。

## 【 0 0 2 5 】

請求項 1 3 に係る暗号通信方法は、センタから各エンティティへ各エンティティの秘密鍵を送付し、一方のエンティティが前記センタから送付された自身の秘密鍵と他方のエンティティの公開鍵とから求めた共通鍵を用いて平文を暗号文に暗号化して前記他方のエンティティへ伝送し、前記他方のエンティティが伝送された暗号文を、前記センタから送付された自身の秘密鍵と前記一方のエンティティの公開鍵とから求めた、前記共通鍵と同一の共通鍵を用いて平文に復号するこ

とにより、エンティティ間で情報の通信を行う暗号通信方法において、各エンティティを特定する特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティの特定情報に基づき代数曲線上の点に写像したものを各エンティティの公開鍵とすることを特徴とする。

## 【 0 0 2 6 】

請求項 1 4 に係る秘密鍵生成器は、エンティティを特定する特定情報に基づいて前記エンティティの秘密鍵を生成する生成器において、前記エンティティの特定情報に基づき代数曲線上の点に写像して写像値を得る手段と、該写像値と秘密情報とを用いて前記秘密鍵を生成する手段とを備えることを特徴とする。

## 【 0 0 2 7 】

請求項 1 5 に係る共通鍵生成器は、一方のエンティティを特定する特定情報に基づく秘密鍵と通信相手の他方のエンティティを特定する特定情報に基づく公開鍵とから共通鍵を生成する生成器において、前記他方のエンティティの特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得る手段と、該写像値と前記秘密鍵とを用いて前記共通鍵を生成する手段とを備えることを特徴とする。

## 【 0 0 2 8 】

請求項 1 6 に係る暗号通信システムは、送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を平文に復号する復号処理を、複数のエンティティ間で相互に行うこととし、各エンティティを特定する特定情報に基づいて各エンティティの秘密鍵を生成して各エンティティへ送付するセンタと、該センタから送付された自身の秘密鍵と通信対象のエンティティの特定情報に基づく公開鍵とを用いて前記暗号化処理及び復号処理に使用する共通鍵を生成する複数のエンティティとを有する暗号通信システムにおいて、前記センタにて、各エンティティの特定情報に基づき代数曲線上の点に写像したものと前記センタ固有の秘密情報とを用いて各エンティティの秘密鍵を生成し、各エンティティにて、通信対象のエンティティの特定情報に基づき代数曲線上の点に写像したものを前記公開鍵として前記共通鍵を生成するようにしたことを特徴とする。

## 【 0 0 2 9 】

請求項 1 7 に係る記録媒体は、コンピュータにエンティティの秘密鍵を生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と秘密情報とを用いて前記秘密鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする。

## 【 0 0 3 0 】

請求項 1 8 に係る記録媒体は、コンピュータに、暗号通信システムにおける平文から暗号文への暗号化処理及び暗号文から平文への復号処理に使用する共通鍵を第 1 エンティティ側で生成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記第 1 エンティティの秘密鍵を入力することをコンピュータに実行させるプログラムコード手段と、通信相手の第 2 エンティティを特定する特定情報に基づき代数曲線上の点に写像して前記公開鍵としての写像値を得ることをコンピュータに実行させるプログラムコード手段と、前記写像値と入力した前記秘密鍵とを用いて前記共通鍵を生成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されていることを特徴とする。

## 【 0 0 3 1 】

本発明では、各エンティティの特定情報（ID 情報）に基づいて、楕円暗号で利用されている楕円曲線，超楕円曲線等の代数曲線上の点に写像し、その写像値を各エンティティの公開鍵とする。この代数曲線及び写像のアルゴリズムは公開する。センタでは、各エンティティの特定情報（ID 情報）に基づき代数曲線上の点に写像し、その写像値とセンタ自身の秘密情報とを用いて、各エンティティ固有の秘密鍵を生成し、これを対応するエンティティへ秘密裏に送付する。各エンティティは、センタから送られる自身固有の秘密鍵と、通信相手の特定情報（ID 情報）に基づき代数曲線上の点に写像した写像値とを用いて、暗号化処理・復号処理に用いる共通鍵を生成する。この際、楕円曲線上で定義されるペアリン

グ（バイユ（Weil）ペアリング，テイト（Tate）ペアリング等）を利用して、予備通信を行うことなく、両エンティティ間で同一の共通鍵を共有する。本発明における代数曲線上の点への写像は、各エンティティ，センタの何れでも可能である。

### 【0032】

本発明では、安全性の根拠を代数曲線上の離散対数問題（例えば楕円曲線上の離散対数問題、以下、これを単に楕円離散対数問題という）に置いている。複数のエンティティによる結託攻撃にて本発明の暗号システムが破られることは、例えば楕円離散対数問題が解かれることと等価であるかまたはそれ以上に困難であり、その安全性は極めて高い。

### 【0033】

#### 【発明の実施の形態】

本発明の実施の形態について具体的に説明する。

図1は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できるセンタ1が設定されており、このセンタ1としては、例えば社会の公的機関を該当できる。このセンタ1と、この暗号通信システムを利用するユーザとしての複数の各エンティティA，B，…，Zとは、秘密通信路2a，2b，…，2zにより接続されており、これらの秘密通信路2a，2b，…，2zを介してセンタ1から秘密の鍵情報（秘密鍵 $S_a$ ， $S_b$ ，…， $S_z$ ）が各エンティティA，B，…，Zへ伝送されるようになっている。また、2人のエンティティの間には通信路3ab，3az，3bz，…が設けられており、この通信路3ab，3az，3bz，…を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

### 【0034】

以下、代数曲線として楕円曲線を用いる場合の本発明における基本方式について説明する。

まず、本発明で用いる楕円曲線のバイユペアリングの基本的性質を述べる。バイユペアリングは、楕円曲線上の点がなす群 $E/F_q$ から有限体上 $F_d$ （但し、 $d = q^k$ ）の乗法群への写像である。バイユペアリングには、以下に示すよう双



線形性と交換則とが成り立つ。なお、 $(\cdot)$  はバイユペアリングを表し、 $P, P_1, P_2, Q, Q_1, Q_2$  は楕円曲線上の点を示す。

【0035】

(双線形性)

$$(P_1 + P_2 \cdot Q) = (P_1 \cdot Q) (P_2 \cdot Q)$$

$$(P \cdot Q_1 + Q_2) = (P \cdot Q_1) (P \cdot Q_2)$$

(交換則)

$$(P \cdot Q) = (Q \cdot P)^{-1}$$

双線形性を有するので、 $m$  を整数とした場合、以下のような等式が成立する。

$$(mP \cdot Q) = (P \cdot Q)^m$$

$$(P \cdot mQ) = (P \cdot Q)^m$$

【0036】

バイユペアリングに基づく鍵共有法を以下に説明する。

(センタ1での秘密鍵生成)

任意のエンティティAの名前、住所、電話番号、メールアドレス等の特定情報(ID情報)を $ID_a$ とする。センタ1は、バイユペアリングのアルゴリズム $(\cdot)$ と任意のエンティティAのID情報 $ID_a$ を楕円曲線上の点 $P_a \in E/F_q$ に変換して(写像して)公開鍵を求める関数 $f(\cdot)$ とを公開する。また、センタ1は、秘密の乱数 $r$ を生成し、この乱数 $r$ とエンティティAの公開鍵 $P_a$ とを用いて下記(1)のようにエンティティAの秘密鍵 $S_a$ を求め、求めた秘密鍵 $S_a$ を秘密裏にエンティティAへ配布する。

$$S_a = r P_a \quad \dots (1)$$

【0037】

以上のような秘密情報、公開情報をまとめると、次のようになる。

センタ1の公開情報 :  $(\cdot), f(\cdot)$

センタ1の秘密情報 :  $r$  (ランダムな整数)

エンティティAの公開鍵 :  $P_a (= f(ID_a))$

エンティティAの秘密鍵 :  $S_a (= r \cdot f(ID_a))$

【0038】

(エンティティ A, B での共通鍵生成)

各エンティティは、センタ 1 から配布された自身の秘密鍵と通信相手であるエンティティの公開鍵とから、楕円曲線上でのバイユペアリングを利用して、共通鍵を生成する。

(第 1 例)

エンティティ A の ID 情報  $ID_a$  とエンティティ B の ID 情報  $ID_b$  との間での大小比較を行えるアルゴリズムを設定し、ペアリングを計算する際にその大小情報を用いてペアリングの順序を適切に設定する。このアルゴリズムとしては、辞書式または 2 進数で表したときの大小などが可能である。なお、ペアリングの順序を設定する方法として、ID 情報  $ID_a$ ,  $ID_b$  を変換 (写像) した後の公開鍵  $P_a$ ,  $P_b$  の大小情報を用いることも可能である。

【0039】

例えば、 $ID_a > ID_b$  である場合、エンティティ A は、自身の秘密鍵  $S_a$  と、エンティティ B の ID 情報  $ID_b$  を楕円曲線に写像した公開鍵  $P_b$  とを用いて、下記 (2) に従って共通鍵  $K_{ab}$  を生成する。

$$\begin{aligned} K_{ab} &= (S_a \cdot P_b) \\ &= (r P_a \cdot P_b) \\ &= (P_a \cdot P_b)^r \quad \dots (2) \end{aligned}$$

【0040】

一方、 $ID_a > ID_b$  である場合、エンティティ B は、エンティティ A の ID 情報  $ID_a$  を楕円曲線に写像した公開鍵  $P_a$  と自身の秘密鍵  $S_b$  とを用いて、下記 (3) に従って共通鍵  $K_{ba}$  を生成する。

$$\begin{aligned} K_{ba} &= (P_a \cdot S_b) \\ &= (P_a \cdot r P_b) \\ &= (P_a \cdot P_b)^r \quad \dots (3) \end{aligned}$$

よって、エンティティ A が生成する共通鍵  $K_{ab}$  とエンティティ B が生成する共通鍵  $K_{ba}$  とは一致して、両エンティティ A, B 間で共通鍵を共有できる。

【0041】

以下に、上記のような ID 情報の大小関係を設定しないで鍵共有を可能とする

2つの例について説明する。

【0042】

(第2例)

$x, y$ に関する対称関数  $g(x, y)$  (但し、 $g(x, y) = xy$ は除く)を設定する。以下の例では、 $g(x, y) = x + y$ とする。エンティティAは、 $g(x, y) = x + y$ に従って下記(4)のように、共通鍵  $K_{ab} = k_{ab} + k_{ba}$ を生成する。

$$\begin{aligned} K_{ab} &= k_{ab} + k_{ba} \\ &= (S_a \cdot P_b) + (P_b \cdot S_a) \\ &= (r P_a \cdot P_b) + (P_b \cdot r P_a) \\ &= (P_a \cdot P_b)^r + (P_b \cdot P_a)^r \quad \dots (4) \end{aligned}$$

【0043】

一方、エンティティBは、 $g(x, y) = x + y$ に従って下記(5)のように、共通鍵  $K_{ba} = k_{ba} + k_{ab}$ を生成する。

$$\begin{aligned} K_{ba} &= k_{ba} + k_{ab} \\ &= (S_b \cdot P_a) + (P_a \cdot S_b) \\ &= (r P_b \cdot P_a) + (P_a \cdot r P_b) \\ &= (P_b \cdot P_a)^r + (P_a \cdot P_b)^r \quad \dots (5) \end{aligned}$$

よって、エンティティAが生成する共通鍵  $K_{ab}$ とエンティティBが生成する共通鍵  $K_{ba}$ とは一致して、両エンティティA, B間で共通鍵を共有できる。なお、他の種類の対称関数  $g(x, y)$ を利用して、同様に鍵共有が可能である。

【0044】

(第3例)

エンティティAは、第2例で示した  $k_{ab}$ を用いて、下記(6)のように、共通鍵  $K_{ba} = k_{ab} + k_{ab}^{-1}$ を生成する。

$$\begin{aligned} K_{ba} &= k_{ab} + k_{ab}^{-1} \\ &= (S_a \cdot P_b) + (S_a \cdot P_b)^{-1} \\ &= (r P_a \cdot P_b) + (r P_a \cdot P_b)^{-1} \\ &= (P_a \cdot P_b)^r + (P_a \cdot P_b)^{-r} \quad \dots (6) \end{aligned}$$

## 【 0 0 4 5 】

エンティティ B は、第 2 例で示した  $k_{ba}$  を用いて、下記 (7) のように、共通鍵  $K_{ba} = k_{ba} + k_{ba}^{-1}$  を生成する。

$$\begin{aligned}
 K_{ba} &= k_{ba} + k_{ba}^{-1} \\
 &= (S_b \cdot P_a) + (S_b \cdot P_a)^{-1} \\
 &= (r P_b \cdot P_a) + (r P_b \cdot P_a)^{-1} \\
 &= (P_b \cdot P_a)^r + (P_b \cdot P_a)^{-r} \\
 &= (P_a \cdot P_b)^{-r} + (P_a \cdot P_b)^r \quad \dots (7)
 \end{aligned}$$

よって、エンティティ A が生成する共通鍵  $K_{ab}$  とエンティティ B が生成する共通鍵  $K_{ba}$  とは一致して、両エンティティ A, B 間で共通鍵を共有できる。

## 【 0 0 4 6 】

以上のようにして、バイユペアリングを利用して、各エンティティ間で等しい共通鍵を容易に生成できる。

## 【 0 0 4 7 】

なお、上述した例では、エンティティ A の ID 情報  $ID_a$  から直接に写像点  $P_a$  を求めるようにしたが、一方向性関数を用いて ID 情報  $ID_a$  を変換し、その変換値から写像点  $P_a$  を求めるようにしても良い。この際、一方向性関数の例としてハッシュ関数  $h()$  を用いた場合、公開鍵  $P_a = f(h(ID_a))$ 、秘密鍵  $S_a = r \cdot f(h(ID_a))$  となる。

## 【 0 0 4 8 】

エンティティが、センタ 1 の秘密情報  $r$  を求めることを困難にするためには、次の 2 つの条件が必要である。

(条件 1)  $q$  を  $2^{160}$  以上に設定すること。

(条件 2)  $\#E/F_q \mid q^k - 1$  かつ  $q^k > 2^{1024}$  を満たすような整数  $k$  が存在すること。

## 【 0 0 4 9 】

(条件 1) は、楕円離散対数問題を求めることを困難にするために必要である。(条件 2) は、有限体  $F_d$  (但し、 $d = q^k$ ) の離散対数問題を求めることを困難にするために必要である。

## 【0050】

次に、上述した鍵共有方式を利用した暗号システムにおけるエンティティ間の情報通信について説明する。図2は、2人のエンティティA、B間における情報の通信状態を示す模式図である。図2の例は、エンティティAが平文（メッセージ）Mを暗号文Cに暗号化してそれをエンティティBへ伝送し、エンティティBがその暗号文Cを元の平文（メッセージ）Mに復号する場合を示している。

## 【0051】

センタ1には、関数  $f()$  を用いて、各エンティティA、BのID情報  $ID_a$ 、 $ID_b$  を楕円曲線に写像した写像位置である公開鍵  $P_a$ 、 $P_b$  を得る公開鍵生成器1aと、その公開鍵  $P_a$ 、 $P_b$  とセンタ固有の秘密情報  $r$  とを用いて各エンティティA、Bの秘密鍵  $S_a$ 、 $S_b$  を求める秘密鍵生成器1bとが備えられている。そして、センタ1から各エンティティA、Bへ、前記(1)に従って生成された秘密鍵  $S_a$ 、 $S_b$  が送付される。

## 【0052】

エンティティA側には、エンティティBのID情報  $ID_b$  を入力し、それを楕円曲線に写像した写像位置である公開鍵  $P_b$  を得る公開鍵生成器11と、センタ1から送られる秘密鍵  $S_a$  と公開鍵生成器11からの公開鍵  $P_b$  とに基づいてエンティティAが求めるエンティティBとの共通鍵  $K_{ab}$  を生成する共通鍵生成器12と、共通鍵  $K_{ab}$  を使用して平文（メッセージ）Mを暗号文Cに暗号化して通信路30へ出力する暗号化器13とが備えられている。

## 【0053】

また、エンティティB側には、エンティティAのID情報  $ID_a$  を入力し、それを楕円曲線に写像した写像位置である公開鍵  $P_a$  を得る公開鍵生成器21と、センタ1から送られる秘密鍵  $S_b$  と公開鍵生成器21からの公開  $P_a$  とに基づいてエンティティBが求めるエンティティAとの共通鍵  $K_{ba}$  を生成する共通鍵生成器22と、通信路30から入力した暗号文Cを共通鍵  $K_{ba}$  を使用して平文（メッセージ）Mに復号して出力する復号器23とが備えられている。

## 【0054】

次に、動作について説明する。エンティティAからエンティティBへ情報を伝

送しようとする場合、まず、エンティティ B の ID 情報  $ID_b$  が公開鍵生成器 1 1 に入力されて公開鍵  $P_b$  が得られ、得られた公開鍵  $P_b$  が共通鍵生成器 1 2 へ送られる。また、センタ 1 から秘密鍵  $S_a$  が共通鍵生成器 1 2 へ入力される。そして、前記 (2), (4) または (6) に従って共通鍵  $K_{ab}$  が求められて、暗号化器 1 3 へ送られる。暗号化器 1 3 において、この共通鍵  $K_{ab}$  を用いて平文 (メッセージ)  $M$  が暗号文  $C$  に暗号化され、暗号文  $C$  が通信路 3 0 を介して伝送される。

## 【0055】

通信路 3 0 を伝送された暗号文  $C$  はエンティティ B の復号器 2 3 へ入力される。エンティティ A の ID 情報  $ID_a$  が公開鍵生成器 2 1 に入力されて公開鍵  $P_a$  が得られ、得られた公開鍵  $P_a$  が共通鍵生成器 2 2 へ送られる。また、センタ 1 から秘密鍵  $S_b$  が共通鍵生成器 2 2 へ入力される。そして、前記 (3), (5) または (7) に従って共通鍵  $K_{ba}$  が求められて、復号器 2 3 へ送られる。復号器 2 3 において、この共通鍵  $K_{ba}$  を用いて暗号文  $C$  が平文 (メッセージ)  $M$  に復号される。

## 【0056】

次に、本発明における安全性について説明する。本発明の安全性は、楕円離散対数問題と後述するようにこれと等価である拡張楕円離散対数問題とに基づいている。

## 【0057】

〔楕円離散対数問題と拡張楕円離散対数問題との等価性〕

通常の楕円離散対数問題とは、楕円曲線  $E$  上の任意の点  $P$  とその  $r$  倍点  $Q = rP$  が与えられている場合に、 $P, Q$  から  $r$  を求める問題である。ここで、下記 (8) のように、楕円曲線上の任意の点  $P_i$  ( $1 \leq i \leq n-1$ ) とその点  $P_i$  に基づく  $Q$  が与えられている場合に、ある 1 組の  $r_i$  ( $1 \leq i \leq n-1$ ) を求める問題を拡張楕円離散対数問題と定義する。楕円離散対数問題と拡張楕円離散対数問題との等価性について考察する。なお、議論の簡単化のために楕円曲線は素数位数  $p$  とする。

## 【0058】

【数 1】

$$P_i, Q (= \sum_{i=1}^{n-1} r_i P_i) \rightarrow r_i \quad (1 \leq i \leq n-1) \cdots (8)$$

【0059】

(楕円離散対数問題から拡張楕円離散対数問題への帰着)

楕円離散対数問題がベースポイント  $P$  を基準として解けると仮定する。 $P_i$  ( $1 \leq i \leq n-1$ ) 及び  $Q$  は、夫々楕円曲線上のベースポイント  $P$  を基準として係数を、下記 (9) のように求めることができる。

【0060】

【数 2】

$$\begin{aligned} P_i &\rightarrow r'_i \quad \text{但し } P_i = r'_i P \quad (1 \leq i \leq n-1) \\ \sum_{i=1}^{n-1} r_i P_i &\rightarrow r' \quad \text{但し } \sum_{i=1}^{n-1} r_i P_i = r' P \quad \cdots (9) \end{aligned}$$

【0061】

係数  $r'_i$ ,  $r'$  を  $F_p$  の元として、下記 (10) の不定方程式を解くことにより、 $r_i$  ( $1 \leq i \leq n-1$ ) を求めることが可能である。よって、拡張楕円離散対数問題を解くことができる。

【0062】

【数 3】

$$r' = \sum_{i=1}^{n-1} r_i r'_i \quad \cdots (10)$$

【0063】

(拡張楕円離散対数問題から楕円離散対数問題への帰着)

任意の拡張楕円離散対数問題が解けると仮定する。ここで、楕円曲線上の点  $P_i$  ( $1 \leq i \leq n$ ) に対して、下記 (11) で示される拡張楕円離散対数問題を解き

、これを行列を用いて表すと下記 (12) のようになる。

【0064】

【数4】

$$P_i = \sum_{\substack{j=1 \\ j \neq i}}^n r_{i,j} P_j \quad (1 \leq i \leq n) \cdots (11)$$

$$\begin{pmatrix} r_{1,1}P_1 & r_{1,2}P_2 & \cdots & r_{1,n-1}P_{n-1} & -P_n \\ r_{2,1}P_1 & r_{2,2}P_2 & \cdots & -P_{n-1} & r_{2,n}P_n \\ \vdots & \vdots & & \vdots & \vdots \\ -P_1 & r_{n,2}P_2 & \cdots & r_{n,n-1}P_{n-1} & r_{n,n}P_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdots (12)$$

【0065】

上記 (12) の行列について係数のみを抜き出すと下記 (13) のような関係式が得られ、下記 (14) のように変形可能である。

【0066】



【数 5】

$$\begin{pmatrix} r_{1,1} & r_{1,2} & \cdots & r_{1,n-1} & -1 \\ r_{2,1} & r_{2,2} & \cdots & -1 & r_{2,n} \\ \vdots & \vdots & & \vdots & \vdots \\ -1 & r_{n,2} & \cdots & r_{n,n-1} & r_{n,n} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{p} \quad \cdots (13)$$

$$\begin{pmatrix} -1 & 0 & \cdots & 0 & r'_1 \\ 0 & -1 & \cdots & 0 & r'_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & r'_{n-1} \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \pmod{p} \quad \cdots (14)$$

【0067】

上記 (14) から分かるように、点  $P_i$  ( $1 \leq i \leq n-1$ ) は  $P_n$  の定数倍で表すことが可能である。即ち、拡張楕円離散対数問題を解くことによって、 $P_i = r'_i \cdot P_n$  を満たす  $r'_i$  を求めることができる。

以上のことから、楕円離散対数問題と拡張楕円離散対数問題とは等価になる。

【0068】

〔センタの秘密情報に関する安全性〕

エンティティ C の公開鍵  $P_c$  と秘密鍵  $S_c$  とからセンタの秘密情報  $r$  を得ることは、楕円離散対数問題を解くことと等価であって、困難である。

エンティティ A の公開鍵  $P_a$  とエンティティ B の公開鍵  $P_b$  とから  $(P_a \cdot P_b)$  を計算し、これと共通鍵  $K_{ab} = (P_a \cdot P_b)^r$  とから  $r$  を得ることは離散対数問題を解くことと等価であって、困難である。

よって、どのエンティティもセンタの秘密情報  $r$  を求めることができない。

【0069】

〔エンティティの秘密鍵に関する安全性〕

$n$  人のエンティティが結託してエンティティ C の秘密鍵  $S_c$  を偽造する攻撃に

について考察する。エンティティ C の公開鍵  $P_c$  が下記 (15) のように他のエンティティの公開鍵の線形結合によって表すことが可能であると仮定すると、前記 (1) にこの線形結合を代入すると、下記 (16) の関係式が成立するので、エンティティ C の秘密鍵  $S_c$  が露呈する。

$$P_c = u_1 P_1 + u_2 P_2 + \cdots + u_n P_n \quad \cdots (15)$$

$$\begin{aligned} S_c &= r P_c \\ &= r (u_1 P_1 + u_2 P_2 + \cdots + u_n P_n) \\ &= u_1 (r P_1) + u_2 (r P_2) + \cdots + u_n (r P_n) \\ &= u_1 S_1 + u_2 S_2 + \cdots + u_n S_n \quad \cdots (16) \end{aligned}$$

【0070】

しかし、上記 (15) での係数  $u_i$  を得るには拡張楕円離散対数問題を解く必要があり、このような攻撃は困難であるといえる。よって、安全性は拡張楕円離散対数問題を解くことの難しさに基づいている。

【0071】

ここで、この秘密鍵の安全性について更に詳述する。拡張楕円離散対数問題は、 $P$  を  $E/F_q$  上の任意の点、 $(G_1, G_2)$  を  $E/F_q$  の生成元とした場合に、下記 (17) において係数  $u_1, u_2$  を求める問題である。

$$P = u_1 G_1 + u_2 G_2 \quad \cdots (17)$$

【0072】

$G_1, G_2$  の次数を  $\#(G_1), \#(G_2)$  と定義する。但し、 $\#(G_1) \mid \#(G_2)$  とする。拡張楕円離散対数問題が解けるとすれば、 $P = u_1 G_1 + u_2 G_2$  での係数  $u_1, u_2$  及び  $Q = v_1 G_1 + v_2 G_2$  での係数  $v_1, v_2$  は求まり、楕円離散対数問題  $Q = r P$  は、下記 (18) のように解ける。

【0073】

【数6】

$$rU_1 \equiv V_1 \pmod{\#(G_1)}$$

$$rU_2 \equiv V_2 \pmod{\#(G_2)}$$

$$r \equiv \frac{V_1}{U_1} \left( \pmod{\frac{\#(G_1)}{\gcd(u_1, \#(G_1))}} \right)$$

$$r \equiv \frac{V_2}{U_2} \left( \pmod{\frac{\#(G_2)}{\gcd(u_2, \#(G_2))}} \right) \cdots (18)$$

【0074】

上記(15)を解く問題と拡張楕円離散対数問題との等価性について考察する。

上記(15)が解けたとすると、下記(19)の $r_{i,j}$ を求めることができる。

【0075】

【数7】

$$P_i = \sum_{\substack{j=1 \\ j \neq i}}^n r_{i,j} P_j \quad (1 \leq i \leq n-2) \cdots (19)$$

【0076】

そして、下記(20)の式において、左辺の $(n-2) \times (n-2)$ の行列式が、 $P_{n-1} = G_1$ 、 $P_n = G_2$ である $\#(G_2)$ に素であるという仮定のもとで、その下記(20)の式を解くことができる。行列式が $\#(G_2)$ に素でない場合には、上記(19)の別の解 $r_{i,j}$ を選択できる。

【0077】

【数 8】

$$\begin{pmatrix} -1 & r_{1,2} & \cdots & r_{1,n-2} \\ r_{2,1} & -1 & \cdots & -r_{2,n-2} \\ \vdots & \vdots & & \vdots \\ r_{n-2,1} & r_{n-2,2} & \cdots & -1 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_{n-2} \end{pmatrix} \\ = - \begin{pmatrix} r_{1,n-1} & r_{1,n} \\ r_{2,n-1} & r_{2,n} \\ \vdots & \vdots \\ r_{n-2,n-1} & r_{n-2,n} \end{pmatrix} \begin{pmatrix} P_{n-1} \\ P_n \end{pmatrix} \cdots (20)$$

【0 0 7 8】

この結果、上記 (15) が解けるとすれば、下記 (21) に示す  $P_i$  と  $(G_1, G_2)$  との拡張楕円離散対数問題も解ける。

【0 0 7 9】

【数 9】

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_{n-2} \end{pmatrix} = \begin{pmatrix} r'_{1,n-1} & r'_{1,n} \\ r'_{2,n-1} & r'_{2,n} \\ \vdots & \vdots \\ r'_{n-2,n-1} & r'_{n-2,n} \end{pmatrix} \begin{pmatrix} P_{n-1} \\ P_n \end{pmatrix} \cdots (21)$$

【0 0 8 0】

これとは逆に、拡張楕円離散対数問題が解ければ、上記 (15) が解けることを示す。 $P_i$  と  $(G_1, G_2)$  との拡張楕円離散対数問題を下記 (22) のように定義し、 $P_C$  と  $(G_1, G_2)$  との拡張楕円離散対数問題を下記 (23) のように定義すると、下記 (24) に示すような関係が成立する。

【0 0 8 1】

【数10】

$$\begin{pmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{pmatrix} = \begin{pmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \\ \vdots & \vdots \\ r_{n,1} & r_{n,2} \end{pmatrix} \begin{pmatrix} G_1 \\ G_2 \end{pmatrix} \cdots (22)$$

$$P_c = v_1 G_1 + v_2 G_2 \cdots (23)$$

$$\left. \begin{aligned} v_1 G_1 + v_2 G_2 &= \sum_{i=1}^n u_i r_{i,1} G_1 + \sum_{i=1}^n u_i r_{i,2} G_2 \\ v_1 &= \sum_{i=1}^n u_i r_{i,1} \\ v_2 &= \sum_{i=1}^n u_i r_{i,2} \end{aligned} \right\} \cdots (24)$$

【0082】

$v_j$  と  $r_{i,j}$  が与えられている場合には、 $u_i$  が解けることは明らかである。よって、上記(15)を解く問題と拡張楕円離散対数問題とは等価である。また、楕円曲線の群が周期的である場合、拡張楕円離散対数問題が楕円離散対数問題と等価であることは明らかである。よって、この場合、上記(15)を解く問題は楕円離散対数問題と等価になる。

【0083】

〔エンティティ間の共通鍵に関する安全性〕

$n$ 人のエンティティの結託により、エンティティA、エンティティC間の共通鍵を偽造する攻撃について考察する。エンティティCの公開鍵 $P_c$ が上記(15)のように他のエンティティの公開鍵の線形結合によって表すことが可能であると仮定すると、下記(25)、(26)のように、両エンティティA、C間の共通鍵 $K_{ac}$ 、 $K_{ca}$ が露呈する。エンティティCの秘密鍵 $S_c$ が線形結合により書き表せる場合も同様に考えられる。

【0084】

【数11】

$$\begin{aligned}
 K_{ac} &= (S_a \cdot P_c) \\
 &= (S_a \cdot u_1 P_1 + u_2 P_2 + \cdots + u_n P_n) \\
 &= (S_a \cdot P_1)^{u_1} (S_a \cdot P_2)^{u_2} \cdots (S_a \cdot P_n)^{u_n} \\
 &= K_{a1}^{u_1} K_{a2}^{u_2} \cdots K_{an}^{u_n} \cdots (25)
 \end{aligned}$$

$$K_{ca} = K_{1a}^{-u_1} K_{2a}^{-u_2} \cdots K_{na}^{-u_n} \cdots (26)$$

【0085】

しかしながら、上記(15)での係数 $u_i$ を求めるには拡張楕円離散対数問題を解くことになり、このような攻撃は困難である。

【0086】

もし、エンティティAが自身の公開鍵 $P_a$ ，秘密鍵 $S_a$ から他のエンティティ間の共通鍵 $K_{bc}$ を偽造しようとしても不可能である。なぜなら、秘密鍵 $S_b$ ， $S_c$ はエンティティB，Cの秘密情報であり、それらは秘密情報 $r$ なしでは求められないからである。よって、どのエンティティも共通鍵 $K_{bc}$ を偽造できない。

【0087】

秘密鍵 $S_b$ ， $S_c$ なしに結託エンティティIの秘密鍵 $S_i$ から共通鍵 $K_{bc}$ を求める結託攻撃は、秘密鍵 $S_i$ から秘密鍵 $S_b$ ， $S_c$ を求める場合と同じ問題になる。また、結託エンティティI，J間の共通鍵 $K_{ij}$ から共通鍵 $K_{bc}$ を求める結託攻撃は、センタの秘密情報 $r$ を知らないので、困難な問題となる。共通鍵 $K_{bc}$ を求める問題は、Diffie-Hellman型問題に帰着する。

【0088】

ところで、エンティティAは共通鍵 $K_{ab}$ ， $K_{ac}$ を算出することが可能であるので、共通鍵 $K_{ab}$ ， $K_{ac}$ から共通鍵 $K_{bc}$ を求めることができるのであれば、エンティティAは他エンティティ間の共通鍵を偽造可能である。しかし、このような攻撃法は本発明には適用困難である。

## 【 0 0 8 9 】

以下、本発明の他の実施の形態である、各エンティティの ID 情報をベクトルに拡張した鍵共有方式について説明する。

## 【 0 0 9 0 】

エンティティ A の ID 情報であるベクトル  $P_a$  を下記 (27) のように表す。

$$\text{ベクトル } P_a = (P_{a1}, P_{a2}, \dots, P_{an}) \quad \dots (27)$$

また、センタ 1 の秘密情報として  $n \times n$  の対称行列  $R$  を下記 (28) のように設定する。

## 【 0 0 9 1 】

## 【数 1 2】

$$\begin{aligned} R &= R^t \\ &= \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix} \quad \dots (28) \end{aligned}$$

## 【 0 0 9 2 】

センタ 1 は、このベクトル  $P_a$  及び対称行列  $R$  を用い、下記 (29) に従って、エンティティ A の秘密鍵 (ベクトル  $S_a$ ) を求め、求めた秘密鍵を秘密裏にエンティティ A へ送付する。

## 【 0 0 9 3 】

## 【数 1 3】

$$\overrightarrow{S_a} = \overrightarrow{P_a} R \quad \dots (29)$$

## 【 0 0 9 4 】

エンティティ A は、エンティティ B との共通鍵を、下記 (30) に従って、共通鍵  $K_{ab}$  を生成する。但し、点と点との積はバイユペアリングの値とする。

## 【 0 0 9 5 】

【数 14】

$$\begin{aligned}
& K_{ab} \\
&= \overrightarrow{S_a} \xrightarrow{P_b} t \\
&= \overrightarrow{P_a} R \xrightarrow{P_b} t \\
&= (P_{a1} P_{a2} \cdots P_{an}) \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{pmatrix} \begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\
&= \left( \sum_{i=1}^n r_{i1} P_{ai} \quad \sum_{i=1}^n r_{i2} P_{ai} \quad \cdots \quad \sum_{i=1}^n r_{in} P_{ai} \right) \begin{pmatrix} P_{b1} \\ P_{b2} \\ \vdots \\ P_{bn} \end{pmatrix} \\
&= \prod_{j=1}^n \left( \sum_{i=1}^n r_{ij} P_{ai} \cdot P_{bj} \right) \\
&= \prod_{j=1}^n \prod_{i=1}^n (P_{ai} \cdot P_{bj})^{r_{ij}} \quad \cdots (30)
\end{aligned}$$

【0096】

また、エンティティ B は、エンティティ A との共通鍵  $K_{ba}$  を同様に生成する。  
 そして、前述した実施の形態の第 1 例のように各エンティティ A、B 間の ID 情報の大小関係を考慮するようにした場合には、 $K_{ab} = K_{ba}$  となり、同一の共通鍵を共有し合うことができる。

【0097】

次に、この実施の形態における安全性について考察する。

〔センタの秘密情報に関する安全性〕

エンティティ C の公開鍵ベクトル  $P_c$  と秘密鍵ベクトル  $S_c$  とからセンタの秘密行列 R を得ることは、拡張楕円離散対数問題を解くことと等価であって、困難である。

エンティティ A の公開鍵ベクトル  $P_a$  とエンティティ B の公開鍵ベクトル  $P_b$



とから  $(P_{ai} \cdot P_{bj})$  ( $1 \leq i, j \leq n$ ) を計算し、これと下記 (31) に示す共通鍵  $K_{ab}$  とから行列  $R$  の各成分  $r_{ij}$  ( $1 \leq i, j \leq n$ ) を得ることは、拡張楕円離散対数問題が楕円離散対数問題とが等価であることと同様に、拡張離散対数問題と離散対数問題とで等価である。

【0098】

【数15】

$$K_{ab} = \prod_{j=1}^n \prod_{i=1}^n (P_{ai} \cdot P_{bj})^{r_{ij}} \quad \dots (31)$$

【0099】

以上のことから、センタ1の秘密情報（対称行列  $R$ ）は露呈しない。

【0100】

〔エンティティの秘密鍵に関する安全性〕

$n$  人のエンティティが結託してエンティティ  $C$  の秘密鍵ベクトル  $S_c$  を偽造する攻撃について考察する。エンティティ  $C$  の公開鍵ベクトル  $P_c$  が下記 (32) のように他のエンティティの公開鍵ベクトルの線形結合によって表すことが可能であると仮定すると、前記 (29) にこの線形結合を代入すると、下記 (33) の関係式が成立するので、エンティティ  $C$  の秘密鍵ベクトル  $S_c$  が露呈する。

【0101】

【数16】

$$\vec{P}_c = u_1 \vec{P}_1 + u_2 \vec{P}_2 + \cdots + u_n \vec{P}_n \quad \cdots (32)$$

$$\begin{aligned} \vec{S}_c &= \vec{P}_c R \\ &= (u_1 \vec{P}_1 + u_2 \vec{P}_2 + \cdots + u_n \vec{P}_n) R \\ &= u_1 (\vec{P}_1 R) + u_2 (\vec{P}_2 R) + \cdots + u_n (\vec{P}_n R) \\ &= u_1 \vec{S}_1 + u_2 \vec{S}_2 + \cdots + u_n \vec{S}_n \quad \cdots (33) \end{aligned}$$

【0102】

しかし、前記(29)での成分を得るには拡張楕円離散対数問題を解く必要があり、このような攻撃は困難であるといえる。よって、安全性は拡張楕円離散対数問題を解くことの難しさに基づいている。

【0103】

〔エンティティ間の共通鍵に関する安全性〕

n人のエンティティの結託により、エンティティA、エンティティC間の共通鍵を偽造する攻撃について考察する。エンティティCの公開鍵ベクトル $P_c$ が上記(32)のように他のエンティティの公開鍵ベクトルの線形結合によって表すことが可能であると仮定すると、下記(34)、(35)のように、両エンティティA、C間の共通鍵 $K_{ac}$ 、 $K_{ca}$ が露呈する。エンティティCの秘密鍵ベクトル $S_c$ が線形結合により書き表せる場合も同様に考えられる。

【0104】

【数 17】

$$\begin{aligned}
 K_{ac} &= \overrightarrow{S_a} \overrightarrow{P_c} \\
 &= \overrightarrow{S_a} (u_1 \overrightarrow{P_1} + u_2 \overrightarrow{P_2} + \dots + u_n \overrightarrow{P_n}) \\
 &= (\overrightarrow{S_a} \overrightarrow{P_1})^{u_1} (\overrightarrow{S_a} \overrightarrow{P_2})^{u_2} \dots (\overrightarrow{S_a} \overrightarrow{P_n})^{u_n} \\
 &= K_{a1}^{u_1} K_{a2}^{u_2} \dots K_{an}^{u_n} \dots (34)
 \end{aligned}$$

$$K_{ca} = K_{1a}^{-u_1} K_{2a}^{-u_2} \dots K_{na}^{-u_n} \dots (35)$$

【0105】

しかしながら、上記(32)での係数 $u_i$ を求めるには拡張楕円離散対数問題を解くことになり、このような攻撃は困難である。

【0106】

また、この実施の形態にあっても、上述した実施の形態と同様に、あるエンティティが自身の共通鍵から他のエンティティ同士の共通鍵を生成することは困難である。

【0107】

なお、エンティティのID情報を $n \times n$ の対称行列に拡張することも可能である。この場合、共通鍵行列 $k_{ab} = (s_{ij})$ と共通鍵行列 $k_{ba} = (t_{ji})$ とは、下記(36)の関係を満たす。

$$s_{ij} = t_{ji}^{-1} \dots (36)$$

【0108】

なお、上述した例ではバイユペアリングを用いる場合について説明したが、楕円曲線上のペアリングとしてテイト(Tate)ペアリングを利用する場合にあっても、同様に両エンティティ間で鍵共有を行える。

【0109】

また、バイユペアリング及びテイトペアリングの何れの場合にあっても、鍵共有を行う際のペアリング(P, Q)において、点Pの座標と点Qの座標とが異な

る体に属するようにペアリングの計算を拡張することができる。また、点  $P$  の座標を小さな体で定義するとペアリングの計算を高速に行うことができる。

#### 【0110】

楕円曲線の定義体を変更する利点は、確実に共通鍵が 1 とならないようにできるという点、及び、高速に計算できるという点である。楕円曲線の定義体を変更する場合、つまり、2 通りの定義体を用いる場合には、2 通りの公開鍵への対応のさせ方が必要である。従来の ID-NIKS では、エンティティが ID 情報によって決まる 1 通りの公開鍵と自身の秘密鍵とを用いて鍵共有を行っているが、この方式では、ID 情報に基づいて、定義体が異なる同一の楕円曲線上の点へ、2 通りの異なるやり方によって公開鍵を写像し、ID 情報または公開鍵に基づき、一方のエンティティが何れか一方の定義体による公開鍵を使用し、他方のエンティティが他方の定義体による公開鍵を使用して、鍵共有を行う。

#### 【0111】

全エンティティを 2 つのグループ  $G_1$ ,  $G_2$  に分ける。グループ  $G_1$  に属するエンティティは  $P$  を含む群の元を、グループ  $G_2$  に属するエンティティは  $Q$  を含む群の元を夫々 ID 情報として用いることにより、グループ  $G_1$  のエンティティとグループ  $G_2$  のエンティティとにおいて鍵を共有することが可能である。

各エンティティが 2 種類の ID 情報を有しており、エンティティ A とエンティティ B との各 ID 情報に何らかの大小関係を示すアルゴリズムを設定し、何れのエンティティがどちらの ID 情報を使用するかを決定することにより、鍵の共有化を行える。

各エンティティが 2 種類の ID 情報を有しており、両エンティティ間で 2 種類の値を計算し、その 2 つの計算値を足し合わせる等、同じ値になる演算を用いて共通鍵を生成する。

$P$  を含む群の元と  $Q$  を含む群の元との間の変換を適切に定め、その変換をシステム固有の公開情報として用いることにより、鍵の共有化が可能である。

#### 【0112】

なお、上述した例では代数曲線として楕円曲線を用いる場合について説明したが、超楕円曲線を用いる場合にあっても、超楕円離散対数問題及びペアリングを

定義できるので、簡単に拡張することができる。

【0113】

図3は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各エンティティのID情報とセンタ固有の秘密情報とに基づき前述した手法にて各エンティティ固有の秘密鍵を生成する処理（エンティティのID情報に基づき楕円曲線上の点に写像して写像値を得るステップと、その写像値とセンタ固有の秘密情報とを用いて秘密鍵を生成するステップ）を含むか、または、エンティティ自身の秘密鍵と通信相手のエンティティの公開鍵とに基づき前述した手法にて共通鍵を生成する処理（通信相手のエンティティのID情報に基づき楕円曲線上の点に写像して写像値を得るステップと、その写像値とエンティティ自身の秘密鍵とを用いて共通鍵を生成するステップ）を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ40は、センタ1側か、または、各エンティティ側に設けられている。

【0114】

図3において、コンピュータ40とオンライン接続する記録媒体41は、コンピュータ40の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体41には前述の如きプログラム41aが記録されている。記録媒体41から読み出されたプログラム41aがコンピュータ40を制御することにより、各エンティティ固有の秘密鍵を生成するか、または、両エンティティ間の共通鍵を生成する。

【0115】

コンピュータ40の内部に設けられた記録媒体42は、内蔵設置される例えばハードディスクドライブまたはROM等を用いてなり、記録媒体42には前述の如きプログラム42aが記録されている。記録媒体42から読み出されたプログラム42aがコンピュータ40を制御することにより、各エンティティ固有の秘密鍵を生成するか、または、両エンティティ間の共通鍵を生成する。

【0116】

コンピュータ40に設けられたディスクドライブ40aに装填して使用される記録媒体43は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキ

シブルディスク等を用いてなり、記録媒体 4 3 には前述の如きプログラム 4 3 a が記録されている。記録媒体 4 3 から読み出されたプログラム 4 3 a がコンピュータ 4 0 を制御することにより、各エンティティ固有の秘密鍵を生成するか、または、両エンティティ間の共通鍵を生成する。

【0 1 1 7】

【発明の効果】

以上詳述したように、本発明では、各エンティティの ID 情報から生成する公開鍵を楕円曲線上で写像するようにしたので、予備通信を行うことなく両エンティティ間で容易に共通鍵を共有し合うことができる。また、本発明ではその安全性が代数曲線上の離散対数問題に置かれており、結託攻撃などの攻撃に対して強く、ID-NIKS の発展に本発明は寄与できる。

【図面の簡単な説明】

【図 1】

本発明の暗号通信システムの構成を示す模式図である。

【図 2】

2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 3】

記録媒体の実施の形態の構成を示す図である。

【図 4】

ID-NIKS のシステムの原理構成図である。

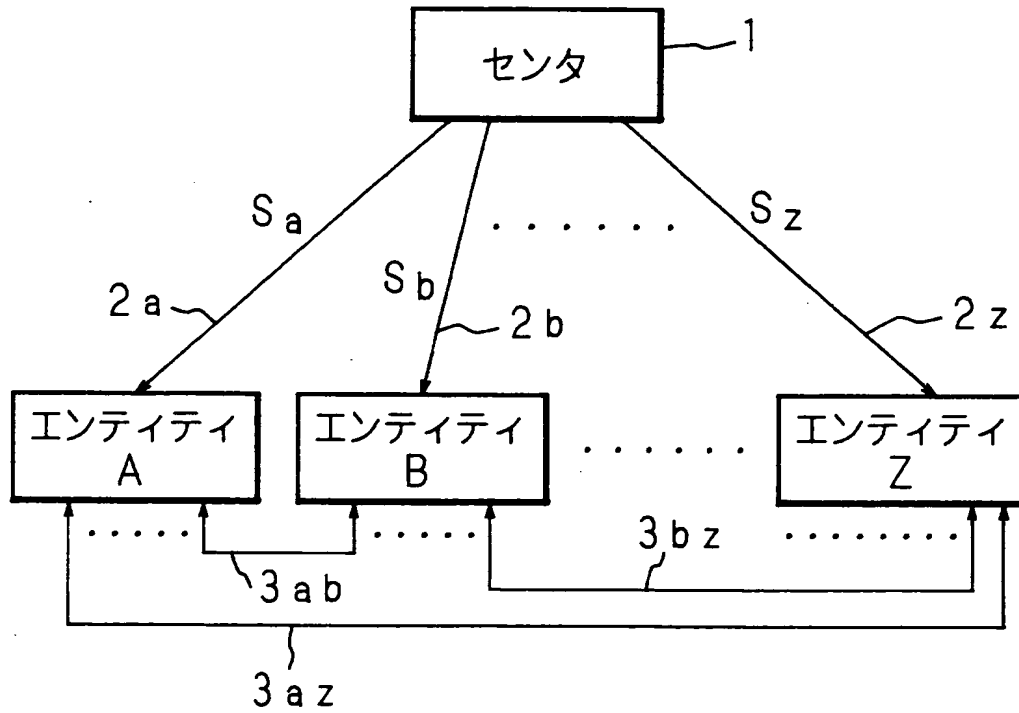
【符号の説明】

- 1 センタ
- 1 1, 2 1 公開鍵生成器
- 1 2, 2 2 共通鍵生成器
- 1 3 暗号化器
- 2 3 復号器
- 3 0 通信路
- 4 0 コンピュータ
- 4 1, 4 2, 4 3 記録媒体

A, B, Z エンティティ

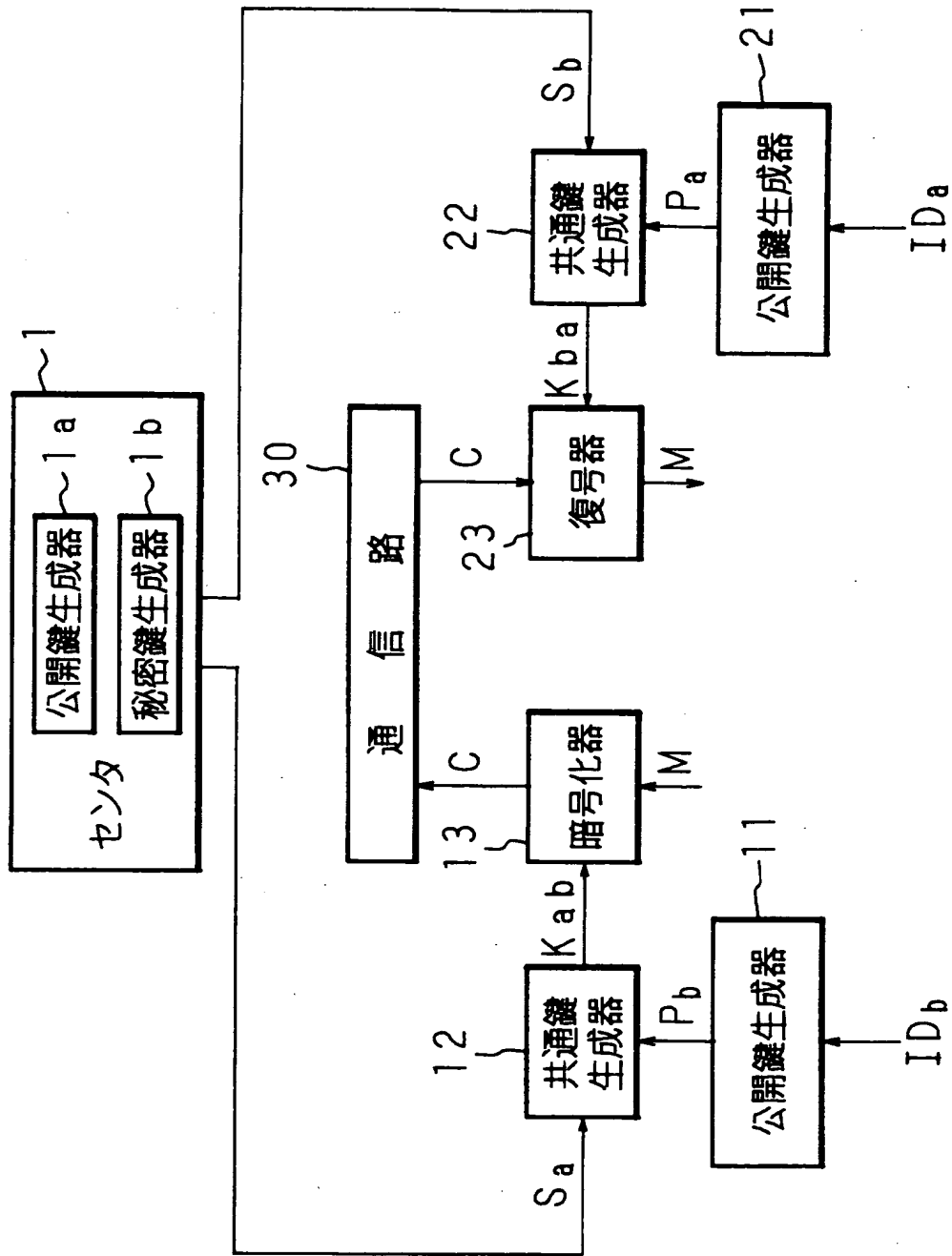
【書類名】 図面

【図 1】





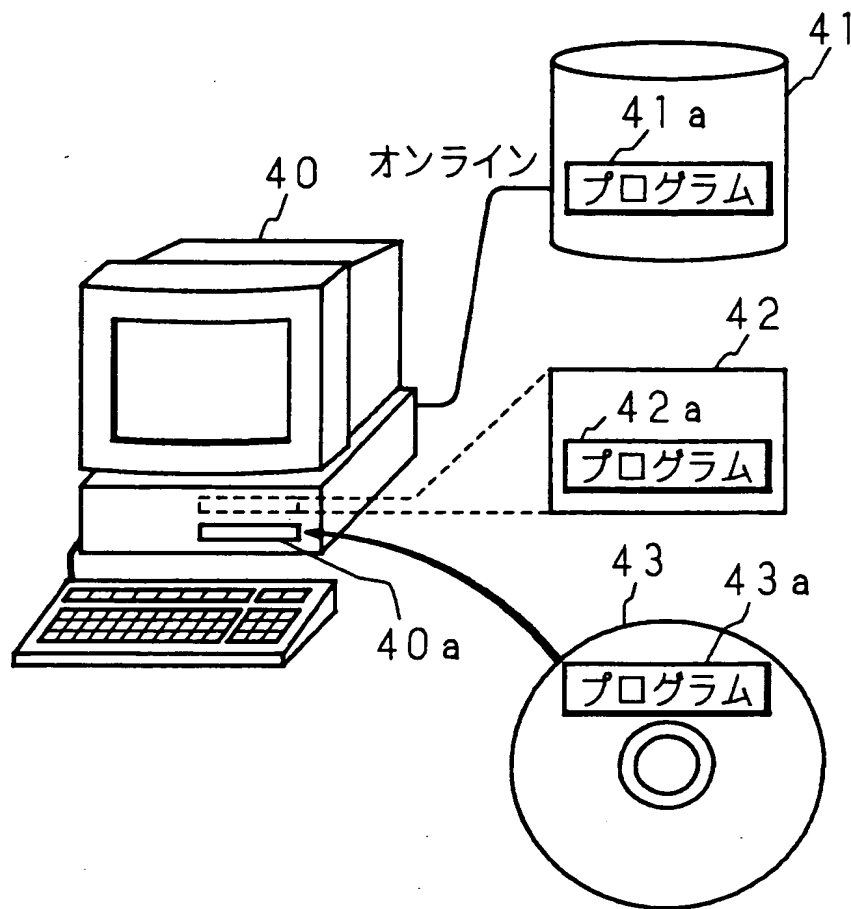
【図 2】



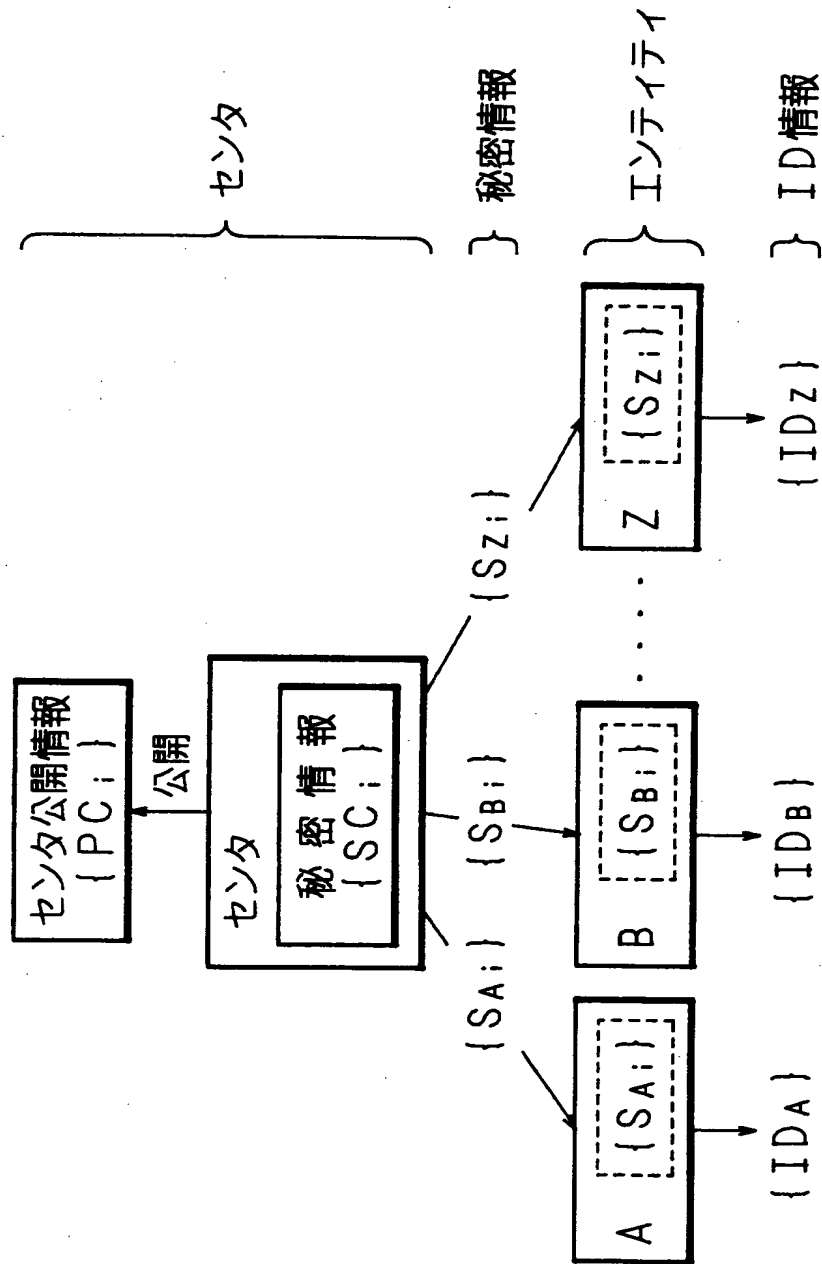
(インティティ A)

(インティティ B)

【図3】



【図 4】



【書類名】            要約書

【要約】

【課題】    両エンティティ間で予備通信を行うことなく容易に共通鍵を共有し合える鍵共有方法、この鍵共有方法に基づいて安全な I D - N I K S を構築できる暗号通信方法及びシステムを提供する。

【解決手段】    センタ 1 は、各エンティティの I D 情報に基づき楕円曲線上の点に写像し、その写像値である公開鍵とセンタ 1 自身の秘密情報とを用いて、各エンティティの秘密鍵を生成する。各エンティティは、センタ 1 から送られる自身の秘密鍵と、通信相手の I D 情報に基づき楕円曲線上の点に写像した写像値である公開鍵とを用いて、暗号化処理・復号処理に用いる共通鍵を生成する。この際、楕円曲線上のペアリングを利用する。

【選択図】            図 1

認定・付加情報

特許出願の番号	特願 2 0 0 0 - 1 3 3 4 7 1
受付番号	5 0 0 0 0 5 5 8 7 6 9
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 2 年 7 月 7 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町 3 番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	599100556
【住所又は居所】	京都府京都市山科区安朱東海道町 1 6 - 2
【氏名又は名称】	境 隆一

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市粟生外院 4 丁目 1 5 番 3 号
【氏名又は名称】	笠原 正雄

【代理人】

申請人

【識別番号】	100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 登夫

【選任した復代理人】

【識別番号】	100114557
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目 4 番 3 号 河野 特許事務所
【氏名又は名称】	河野 英仁

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地  
氏 名 村田機械株式会社

出 願 人 履 歷 情 報

識別番号 [599100556]

1. 変更年月日 1999年 7月16日  
[変更理由] 新規登録  
住 所 京都府京都市山科区四ノ宮柳山町8  
氏 名 境 隆一
2. 変更年月日 2000年 6月14日  
[変更理由] 住所変更  
住 所 京都府京都市山科区安朱東海道町16-2  
氏 名 境 隆一

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日 1997年 1月21日

[変更理由] 新規登録

住 所 大阪府箕面市栗生外院4丁目15番3号

氏 名 笠原 正雄



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**